CHRISTOPHER NEWPORT
UNIVERSITY

GLBA Information Security Program

VERSION 1.0

June 2023

Department: Information Security

Proprietary Statement

This document was developed specifically for and by Christopher Newport University. The concepts and methodologies contained herein are proprietary to Christopher Newport University. Duplication, reproduction, or disclosure of information in this document without the express written consent of Christopher Newport University is prohibited.

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
June 2023	1.0	Initial Plan	Wendy Wilde

TABLE OF CONTENTS

GLBA Information Security Program

OVERVIEW

This document summarizes Christopher Newport University's ("CNU") comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm-Leach-Bliley Act ("GLBA"). In particular, this document addresses the requirements to:

1. Ensure the security and confidentiality of customer information
2. Safeguard against any anticipated threats or hazards to the security or integrity of such information, and
3. Protect against unauthorized access to or use of such information that could substantially harm or inconvenience customers.

The Program incorporates by reference all applicable CNU's policies and procedures with respect to privacy and information security.

SCOPE OF PROGRAM

The Program applies to customer information, which means any nonpublic personal information that CNU or its affiliates handle or maintain about a student, faculty, or staff member or other third party in connection with the provision of a financial service or product by or on behalf of CNU or its affiliates ("GLBA nonpublic financial information (NPI")).

ROLES AND RESPONSIBILITIES

GLBA Program Officer- The designated Qualified Individual "QI" designated to oversee, implement and enforce Christopher Newport University's Information Security Program.

DEFINITIONS

Customer: The GLBA defines "customers" as any person who is provided financial services by the University.

Customer Information: is defined as any record containing nonpublic personal information about a customer, as defined in 16 CFR 313.3(n), whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the University or affiliates.

Information Security Program: As per FTC Safeguard Rules §314.2.c, an Information Security program means the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Financial Product or Service: The term includes student loans, employee loans, activities related to extending credit, financial and investment advisory activities, management consulting and counseling activities, community development activities, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of activities the Federal Trade Commission (FTC) considers a financial product or service:

- Student (or other) loans, including receiving application information, and the making or servicing of such loans
- Collection of delinquent loans and accounts
- Obtaining information from a consumer report

Nonpublic Personal Information "NPI": GLBA defines Non Public Information (NPI) as any financial information given by a consumer to a financial institution for the purpose of obtaining a financial product.

Personal Data: Personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personally Identifiable Information (PII): Any information that relates to an identified or identifiable living individual. Different pieces of information, which can lead to the identification of a particular person, also constitute personal data. Personally Identifiable Financial Information any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain information about a consumer in connection with providing a financial product or service to the consumer.

Protected Information: refers to either personal identifiable information or protected information which is covered by the GLBA.

Third Party: a natural or legal person, public authority, agency, or body other than the data subject, controller, processor and person who under the direct authority of the controller or processor are authorized to process personal data.

ELEMENTS OF THE PROGRAM

1. Designation of Representatives

A. GLBA Program Officer

CNU's Information Security Officer (ISO) is designated as the GLBA Program Officer responsible for coordinating the Program. The GLBA Program Officer is responsible for the development, implementation and oversight of Christopher Newport University's compliance with the policies and procedures required by the Gramm Leach Bliley Act (GBLA) Safeguards Rule.

The GLBA Program Officer may designate other individuals to coordinate particular elements of the Program with the affected departments. The departments of: Information Technology Services, Internal Audit, Admissions, Registrar, Business Office, and Financial Aid will have designated Program representatives and responsibilities. Although ultimate responsibility for compliance lies with the GLBA Program Officer, representatives from each of the operational areas are responsible for implementation and maintenance of the specified requirements of the security program in their departments.

The GLBA Program Officer or designee(s) will work with the University Leadership and the affected department representatives, as necessary, to implement the Program. Questions regarding the implementation of the Program or the interpretation of this document should be directed to the GLBA Program Officer or designee(s) iso@cnu.edu.

B. Affected Departments

Currently, the following departments have been identified as the GLBA-affected areas:

1. Information Technology Services
2. Internal Audit
3. Admissions
4. Registrar
5. Business Office
6. Financial Aid

The GLBA Program Officer or designee will keep records of a periodic review process held at least annually. In addition, the GLBA Program Officer may update the Program from time to time, as appropriate.

C. Affected Department Representative

Each affected CNU department shall appoint a representative, responsible for the GLBA-NPI in that department, to work with the GLBA Program Officer or designee(s) and materially participate in the GLBA Security Governance Committee.

D. GLBA Security Governance Committee

The GLBA Committee exists to ensure that this Information Security Program is kept current and to evaluate potential policy or procedural changes driven by GLBA. Committee membership may change from time-to-time but will minimally include the Information Security Officer, and representatives from: Information Technology Services, Internal Audit, Admission, Registrar, Business Office and Financial Aid. Other individuals may be added as deemed necessary.

Questions regarding GLBA impacts on business processes and policies should be directed to the GLBA Program Officer, and questions regarding technical issues, risk assessments, and information technology security policy should be directed to the GLBA Program Officer or designee(s) iso@cnu.edu.

2. Risk Identification and Assessment

There is an inherent risk in handling and storing any information that must be protected. Identifying areas of risk and maintaining appropriate safeguards can reduce risk. Safeguards are designed to reduce the risk inherent in handling protected information and should include safeguards for information systems and the storage of paper records.

As part of the Program, the GLBA Program Officer or designee will undertake measures that:

1. Identify and assess reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of GLBA NPI that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information; and
2. Assess the sufficiency of any safeguards in place to control these risks.

At a minimum, the risk assessment must consider risks in:

1. Employee training and management;
2. Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
3. Detecting, preventing and responding to attacks, intrusions, or other systems failures.

In implementing the Program, the GLBA Program Officer or designee(s) will coordinate with the affected departments to establish procedures for identifying and assessing such risks in each relevant area of CNU's operations, including the areas noted below.

A. Procedures and Practices

The GLBA Program Officer or designee(s) will coordinate with the affected department representatives to evaluate the effectiveness of the current policies, procedures, and practices of the affected department relating to access to and use of GLBA NPI and to recommend revisions to or development of new policies, procedures, standards, or guidelines, as appropriate.

3. Required Training

GLBA-affected departments handle and have access to protected information in order to perform their job duties. This includes full time, part time, contracted staff and student workers. Departments are responsible for maintaining a high level of awareness and sensitivity to safeguarding protected information and should periodically remind employees of its importance.

The GLBA Program Officer or designee(s) and department representatives are responsible for ensuring that staff are trained in the relevant GLBA concepts and requirements. Training materials relative to GLBA and data handling will be made available to GLBA-affected departments and the training will be a mandatory, annual requirement.

4. Information Systems and Information Processing and Disposal

The GLBA Program Officer or designee(s) will coordinate with the affected department representatives to assess the risks to GLBA NPI associated with CNU's information systems, including, as appropriate, network and software design and information processing, storage, transmission, and disposal of GLBA NPI. The GLBA Program Officer or designee's responsibilities include oversight of University procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

5. Detecting, Preventing, and Responding to Attacks

The GLBA Program Officer or designee(s) will coordinate the evaluation of procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. This includes the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by CNU. The level of monitoring will be appropriate to the potential impact and probability of the identified risks and the sensitivity of the GLBA NPI.

6. Design and Implementation of Safeguards

The GLBA Program Officer or designee(s), will verify that information safeguards are designed and implemented to control the risks identified in the risk assessments set forth above. This review will also confirm that reasonable safeguards and monitoring are implemented by each affected department that has access to GLBA NPI. Such safeguards and monitoring may be accomplished through existing network monitoring, and problem escalation procedures, clean desk processes for paper and other data management practices.

7. Oversight of Third Party Service Providers

Each affected department shall coordinate with those responsible for the third party service procurement activities to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for GLBA NPI to which they will have access.

In addition, the GLBA Program Officer or designee(s) will work with the Office of Procurement Services to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards.

8. Program Adjustments

GLBA mandates that this Information Security Program be subject to periodic review and adjustment. The most frequent of these reviews will occur within the Information Security Policy and Standards. As technologies change and risks evolve, these policies and standards will be periodically reviewed and updated to reflect these changes.

The GLBA Program Officer or designee(s) will evaluate and adjust the Program based on risk identification and assessment activities undertaken to update the Program, as well as any material changes to CNU's technology operations or other circumstances that may have a material impact on the Program.

9. Reports

The GLBA Program Officer will provide an annual Program status report to the University Board of Visitors (BOV). Information to be included in this report may be required from the affected departments.